Audit Report

ENVIRONMENTAL SECURITY YEAR 2000 END-TO-END TESTS

Report No. 99-253 September 15, 1999

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD Home Page at: www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

BOSS	Base Operations Support System
DAISY	Defense Reutilization & Marketing Automated Information System
DLA	Defense Logistics Agency
DLIS	Defense Logistics Information Service
DSS	Distribution Standard System
ERLS	Environmental Reporting Logistics System
HMIS	Hazardous Material Information System
MSDS	Material Safety Data Sheets

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

September 15, 1999

MEMORANDUM FOR DIRECTOR, DEFENSE LOGISTICS AGENCY

SUBJECT: Audit Report on the Environmental Security Year 2000 End-to End Tests (Report No. 99-253)

We are providing this audit report for review and comment.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Because the Director, Defense Logistics Agency did not comment on a draft of this report, we request that the Director, Defense Logistics Agency provide comments on the final report by October 15, 1999.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. William C. Gallagher at (703) 604-9270 (DSN 664-9270) (wgallagher@dodig.osd.mil) or Mr. Robert A. McGriff at (703) 604-9326 (DSN 664-9326) (rmcgriff@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

Robert J Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-253 **September 15, 1999**
(Project No. 9CB-0099)

Audit of the Environmental Security Year 2000 End-to-End Tests

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DOD, to monitor DoD efforts to address the Y2K computing challenge.

Objectives. Our objective was to evaluate the effectiveness of the planned environmental security Y2K end-to-end tests. Specifically, we reviewed the test plans and the results of selected test events for environmental security automated information systems that had been designated as mission-critical by the Defense Logistics Agency, to determine if the tests were adequately planned and executed, and the results adequately documented.

Results. Defense Logistics Agency had not planned and performed effective end–to-end tests for environmental security automated information systems that had been reported as being mission-critical. The tests did not include an adequate number of systems to test the function of environmental reporting. Also, at the time of the audit, the Defense Logistics Agency had not completed system-level contingency plans to address procedures for minimizing disruptions in the event of Y2K related system failures. Insufficiently rigorous end-to-end tests allowed continued risk that the environmental compliance reporting function could be impaired by Y2K related failures. Having sound contingency plans in place therefore is of particular importance in this functional area, whether or not the DoD now considers the systems and function to be other than mission-critical. See the Finding section for additional details.

Summary of Recommendations. We recommend that the Director, Defense Logistics Agency complete system-level contingency plans for environmental security automated information systems.

Management Comments. The Director, Defense Logistics Agency did not submit comments for the draft report dated July 19, 1999. Therefore, we request that the Director, Defense Logistics Agency provide comments in response to the final report by October 15, 1999.

Table of Contents

Introduction

The Office of the Deputy Under Secretary of Defense (Environmental Security) is responsible for global environmental security policy; oversight; advocacy; representation; and implementation of environmental, safety, occupational health, and fire and emergency programs for Defense activities, including the relationship between the environmental and military missions of the Department of Defense. Defense Logistics Agency (DLA) is responsible for Y2K end-to-end mission assessments for environmental security automated information systems by planning and performing end-to-end tests and preparing system-level contingency plans.

Background

Environmental Reporting Requirements. Executive Order No. 12856, August 4, 1993, "Federal Compliance With Right-to-Know Laws and Pollution Prevention Requirements," tasks Federal agencies to become leaders in providing communities and emergency planners with information on hazardous substances and toxic chemicals stored at Government facilities. Executive Order No. 13101, September 14, 1998, "Greening the Government Through Waste Prevention, Recycling, and Federal Acquisition," states that the head of each executive agency shall incorporate waste prevention and recycling into the agency's daily operations, and work to expand markets for recovered materials through greater Federal Government preference and demand for such products. The Executive Orders require agencies to implement cost-effective procurement preference programs favoring purchase of these products and services, and prepare a biennial report to the President on the actions taken to comply with this order.

Environmental Reporting Systems. To comply with Executive Orders No. 12856 and 13101, DLA developed the Environmental Reporting Logistics System (ERLS) to automate the process of collecting and reporting data on hazardous materials. ERLS interfaces with four supporting automated information systems; Base Operations Support System (BOSS), Distribution Standard System (DSS), Defense Reutilization and Marketing Automated Information System (DAISY), and Hazardous Material Information System (HMIS) to track and report on the quantities and location of inventories that contain hazardous materials. See Appendix B for additional details on automated information systems that support the environmental security core function of environmental reporting and Appendix C for details on environmental security system interfaces.

End-to-End Testing. The DoD Year 2000 Management Plan defines end-to-end testing as an assessment of a functional area to determine the Y2K readiness of automated information systems supporting that function. The purpose of end-to-end tests is to give assurance beyond that provided by development, acceptance, and system certification testing.

Mission-critical Systems. The DoD Year 2000 Management Plan requires that systems identified as being critical for warfighting in major theater warfare scenarios be subjected to two operational evaluations or other higher level testing. Other mission-critical systems must be tested in a functional-area end-to-end test or a Service-sponsored Y2K system integration test, unless the systems are not date dependent or stand alone with no interfaces. The DoD Year 2000 Management Plan states that mission-critical systems include those:

- defined by the Information Technology Management Reform Act as National Security Systems;
- identified by the Commanders in Chief which, if not functional, would preclude conducting missions across the full spectrum of operations; or
- required to perform Department-level and Component-level core functions.

DLA designated BOSS, ERLS, and HMIS as mission-critical systems for environmental security. ERLS is the primary tracking and reporting system and is dependent on information provided through interfaces with BOSS, DAISY, DSS, and HMIS to perform the function of environmental compliance reporting.

Capstone Operability Assessment Plan. The Capstone Operability Assessment Plan for Environmental Security Systems Year 2000 Testing, Version 8, April 6, 1999 (draft), establishes guidelines for conducting interoperability assessments, including end-to-end tests, for environmental security systems. This plan defines environmental security systems as those automated information systems that record, collect, and report DoD environmental security corporate information and have external interfaces. The plan states that DLA designated three systems, ERLS, HMIS and BOSS, as mission-critical environmental security systems, and states that those systems and their interfaces will be tested in a major end-to-end mission assessment (the logistics capstone assessment).

Defense Logistics Support Command Year 2000 Management Plan. The DLA Defense Logistics Support Command (DLSC) is responsible for developing guidance for its subordinate commands to implement DoD and DLA Y2K guidance. This plan states that the DLA Chief Information Officer has overall responsibility for the DLA Y2K effort. The plan also states that the primary level field activities of DLSC are responsible for Y2K contingency plans, assessments, certifications, and full participation in end-to-end testing.

Objectives

Our objective was to evaluate the effectiveness of the planned environmental security Y2K end-to-end tests. Specifically, we reviewed the test plans and the results of selected test events for environmental security automated information systems that had been designated as mission-critical by DLA, to determine if the tests were adequately planned and executed, and the results adequately documented. See Appendix A for a discussion of audit scope, methodology, and prior audit coverage.

End-to-End Testing for Environmental Security Systems

The DLA had not planned and performed sufficiently rigorous end-to-end tests for environmental security automated information systems that have been reported by DoD as being mission-critical. The end-to-end tests performed by the Defense Logistics Information Service (DLIS) included only two of the five systems required to perform effective environmental reporting. Also, the DLA had not developed system-level contingency plans for minimizing the risk of mission impairments in the event of Y2K related system failures. This occurred because DLA had not identified, in their test plan, the core processes performed by environmental security systems and interdependencies among those systems. Also, DLA had not developed steps to test the core processes performed by those systems from beginning to end, as required by the DoD Year 2000 Management Plan. At the time of the audit, system-level contingency plans had not been completed. Insufficiently rigorous end-to-end tests allow continued risk that environmental security systems may be impaired by Y2K related failures, resulting in inaccurate environmental reporting. As a result, having sound contingency plans in place for these systems has assumed additional importance.

DoD Year 2000 Management Plan Requirements

The DoD Year 2000 Management Plan, December 1998, states the program's goal is to ensure compliance of a mission-capable force that is able to execute the National Military Strategy, unaffected by failure of mission-critical or support systems to properly process Y2K date-related information. Y2K compliance for system renovation and certification is evaluated from three perspectives: system-level, functional-centric, and mission-centric. The system developer or user was required to perform system renovation, certification, and implementation by December 31, 1998. The Services and agencies are responsible for ensuring that functional-centric testing is performed.

Management Process. The DoD Y2K management process requires DoD managers to:

- prioritize critical missions and functions,
- identify critical information systems and their interfaces,
- identify the interdependencies among systems,
- determine workarounds and alternatives for systems that cannot be made Y2K compliant within established time constraints,

- conduct functional end-to-end tests to ensure the continuity of critical support operations, and

- implement Y2K remedies in a timely and responsible fashion.

Also, DoD managers are responsible for assessing their functional area to determine the Y2K operational readiness of their primary functions. The assessment process will require identification of core processes and the systems and interfaces that they require, as well as an assessment of the readiness of those systems and interfaces to support scheduled Y2K events.

Procedures for Testing Core Functions. The DoD Year 2000 Management Plan requires that all mission-critical automated information systems be tested at least once in a functional Y2K end-to-end test or a Service-sponsored Y2K system integration test. The DoD Year 2000 Management Plan also states that in order to develop end-to-end tests, Components must identify missions and core business processes and the systems required to support those missions. End-to-end tests should be constructed to evaluate the Y2K impact of those systems on a core business process from beginning to end. This testing increases the level of confidence that DoD missions and functions will not be adversely affected by Y2K events.

Procedures for Developing Contingency Plans. Contingency planning is the managerial approach of finding alternative means of satisfying essential requirements, implementing manual processes in the event of outages, and preparing the organization to continue operations in spite of sustained outages of automated information systems. Contingency plans provide insurance against the many possible types of Y2K disruptions by ensuring that plans are in place to expedite restoration of the automated information system and to continue the mission or function while system support is not available. The purpose of the contingency plan is to provide a road map of predetermined actions that will streamline decision making during the contingency and enable resumption of mission operation in a timely and cost-effective manner. Contingency plans must be based on a thorough knowledge of the functions performed by the system, the interdependencies of interacting systems, and the needs of customers and suppliers.

Operational contingency plans detail the procedures by which the mission or function supported by automated information systems will be continued during a prolonged disruption of that support. System-level contingency plans describe the procedures necessary to restore a system in the face of Y2K disruptions. Y2K system-level contingency plans address technical aspects of potential disruptions in systems believed to be Y2K compliant. The sources of these failures may be interface failures, transmission or receipt of corrupt data, failure of utilities or infrastructure, and other Y2K-related failures. Y2K system-level contingency plans are required for all mission-critical systems. Those plans should have been completed by December 31, 1998, and validated with exercises to ensure that they were executable by June 30, 1999.

DLA Year 2000 Preparations

Adequacy of End-to-End Test Plans. DLA had not developed a rigorous plan for end-to-end tests. The DLIS test plan included requirements to test eight dates recommended by the DoD Year 2000 Management Plan, but did not include any steps to test three of the five automated information systems that are needed to perform effective environmental reporting. In accordance with the DoD Year 2000 Management Plan, an end-to-end test must be constructed to evaluate the Y2K impact on a mission or core business process from beginning to end. Activities, missions and functions, and core business processes must be identified during planning, and mapped to the specific automated information systems and interfaces that perform them. The test plan included only ERLS and HMIS and did not include any of the three supporting systems that are required to perform the environmental security core function of environmental reporting. Those supporting systems, BOSS, DAISY and DSS, provide the quantities and location of inventories that contain hazardous materials, and are essential for effective environmental reporting. Also, the test plan did not identify required resources such as personnel, equipment, and funding needed to perform effective end-to-end tests. Effective test plans are needed to ensure that systems will not be impaired by Y2K related failures. See Appendixes B and C for additional information on DLA systems that perform the core function of environmental reporting.

End-to-End Testing. DLA had not performed effective end-to-end tests for environmental security automated information systems. The "Capstone Operability Assessment Plan for Environmental Security Systems Year 2000 Testing" states that the three mission-critical environmental security systems and their interfaces will be tested in a major end-to-end exercise. The purpose of this exercise was to test environmental security automated information systems in performing the core function of environmental reporting. The environmental reporting process requires identification of hazardous compounds in DoD inventories and the amount and location of the inventories that include those hazardous compounds. ERLS, the primary reporting system, pulls information from HMIS to measure the amount of hazardous material contained in compounds. Information on inventory quantities and location is accessed from BOSS, DAISY, and DSS. The documentation for the end-to-end tests showed that DLIS tested only ERLS and HMIS. The tests did not include BOSS, DAISY, or DSS and were, therefore, ineffective in testing the core function of environmental reporting. This occurred because DLA management believed that functional interfaces between ERLS, BOSS, DAISY, and DSS were tested sufficiently during ERLS system development and acceptance testing, as well as system certification testing. However, the DoD Year 2000 Management Plan states that the purpose of end-to-end tests is to give assurance beyond that provided by development, acceptance, and system certification testing. The end-to-end tests should have included an adequate number and mix of automated information systems to test the core process of environmental reporting. At least one of the systems that process inventory information; BOSS, DAISY, or DSS, should be included in end-to-end tests to ensure that the test results are useful. Without effective Y2K end-to-end tests, the risk that environmental security automated information systems may not be able to perform the process of environmental reporting is increased.

Development of System-Level Contingency Plans. The DLA had not developed system-level contingency plans for mission-critical environmental security automated information systems. The DoD Year 2000 Management Plan states that Y2K system-level contingency plans should have been developed for all mission-critical systems by December 31, 1998, and validated with an exercise to ensure that the plans were executable by June 30, 1999. Personnel at DLIS stated, during the audit, that work on contingency plans had only recently been started, and that the draft plan had not been completed. Therefore, the plan was not validated by the deadline established by the DoD Year 2000 Management Plan.

DLA Position on Testing. DLA management stated that environmental security systems and their interfaces had been sufficiently tested during development and system level certification tests. DLA further stated that additional testing of those would be redundant and result in waste of resources.

The purpose of end-to-end testing is to provide assurance that systems will perform their intended missions without Y2K related failures. DLA had no authority to decide unilaterally not to comply with the end-to-end testing requirement in the DoD Y2K Management Plan. This matter was brought to the attention of the Principal Under Secretary of Defense (Acquisition and Technology), who did not support the need for additional testing, and the DLA stated that the systems were actually mission-essential, not mission-critical. We continue to believe that additional testing would have been prudent, whether or not the systems are considered mission-critical. At this late stage, primary focus must turn to the question of whether sound contingency plans are in place.

Summary

The DLA had not planned and performed rigorous end-to-end tests for environmental security automated information systems. The tests did not include an adequate number of systems to test the function of environmental reporting. Also, as of June 1999, DLA had not developed system-level contingency plans to address procedures for minimizing disruptions in the event of Y2K related system failures.

Recommendations

We recommend that the Director, Defense Logistics Agency complete system-level contingency plans for mission-critical environmental security automated information systems.

Management Comments Required

The Director, Defense Logistics Agency did not comment on a draft of this report. We request that the Director, Defense Logistics Agency provide comments on the final report by October 15, 1999.

Appendix A. Audit Process

This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a list of audit projects addressing the issue, see the Y2K web pages on IGNET at http://www.ignet.gov/.

Scope

We evaluated plans and results of end-to-end tests for environmental security systems to determine whether DLA and DLIS had performed effective tests and whether the test results had been adequately documented. We met with management and key operating personnel at DLA, and DLIS and made inquiries to identify the status of their Y2K actions. We compared the end-to-end test to procedures prescribed in the DoD Year 2000 Management Plan issued by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). We reviewed documentation including the inventory of mission-critical environmental security systems and DLA and DLIS contingency plans and continuity of operation plans, and used the information to assess efforts to avoid undue disruption of the environmental security mission.

DoD-wide Corporate Level Government Performance and Results Act Goals. In response to the Government Performance Results Act, the Department of Defense has established 6 DoD-wide corporate level performance objectives and 14 goals for meeting these objectives. This report pertains to achievement of the following objectives and goals.

Objective: Fundamentally reengineer DoD and achieve a 21st century infrastructure. **Goal:** Reduce costs while maintaining required military capabilities across all DoD mission areas. **(DoD-6)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following functional area objectives and goals.

- **Environment Functional Issue Area.** Objective: Achieve compliance with applicable Executive Orders and Federal, State, and inter-state, regional, and local statutory and regulatory environmental requirements. **Goal:** [Reduce] number of new, open, and unresolved enforcement actions applicable [to] environmental statutes. **(ENV-2.1)**

- **Information Technology Management Functional Issue Area. Objective:** Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM-1.2)**

- **Information Technology Management Functional Issue Area. Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate DoD information infrastructure. **(ITM-2.2)**

- **Information Technology Management Functional Issue Area. Objective:** Provide services that satisfy customer information needs. **Goal:** Upgrade technology base. **(ITM-2.3)**

General Accounting Office High Risk Area. The General Accounting Office has identified several high risk areas in the DoD. This report provides coverage of the Information Management and Technology high risk area, within which the Y2K challenge is considered a particularly high risk segment.

Methodology

Audit Type, Dates, and Standards. We performed this program audit from April through June 1999, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We used computer-processed data for this audit, but did not rely on this information to arrive at our audit conclusions.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Management Control Program

We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Summary of Prior Coverage

The General Accounting Office and the Office of the Inspector General, DoD have conducted numerous reviews related to Y2K issues. General Accounting Office reports can be assessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be assessed over the Internet at http://www.dodig.osd.mil.

Appendix B. DLA Systems That Support Environmental Security

Mission-critical Systems

Environmental Reporting Logistics System. The ERLS provides DLA the ability to conform with Executive Orders No. 12856 and 13101, concerning identification and reduction of materials determined to be hazardous. ERLS generates reports on hazardous materials using information from interfaces with two environmental security automated systems, BOSS and HMIS; and two non-environment security systems, DAISY and DSS.

Base Operations Support System. BOSS provides support for local base supply, inventory control, and financial and contracting support. ERLS interfaces with BOSS to obtain information on hazardous material contained in procured items and base inventory. BOSS was developed using an Oracle database and software. BOSS does not perform any date forecasting nor does it do any historical date processing. However, BOSS does store historical data that include dates. DLA made program updates to BOSS to change year formats to a four-position year during the BOSS re-host from a mainframe system to a mid-tier and web application system.

Hazardous Material Information System. HMIS stores Material Safety Data Sheets (MSDS), which provide information such as the amount of hazardous materials contained in chemical compounds and possible safety risks caused by exposure, and other related data for hazardous materials procured by DoD and the General Services Administration.

Other Supporting Systems

Distribution Standard System. DSS manages all functional business processes of DoD warehouse operations. This includes the basic depot processes of receiving, storage, stock selection, packing, shipping and transportation. It also provides processes for functions such as container consolidation point operations, set assembly, inventory, inspection, and workload management.

Defense Reutilization and Marketing Automated Information System. DAISY is an accounting and management system for all property in the Defense Reutilization and Marketing Office (DRMO) inventories. It provides visibility and asset tracking of property for reutilization transfer and donation programs to DoD Federal and State Agencies. It also provides visibility and compliance requirements for hazardous property through the ultimate disposal cycle. DAISY provides management data on all levels of property disposal, which includes historical data, both on line and archived.

APPENDIX C. ERLS System Interfaces

Hazardous Material Inventory Data

ERLS tracks hazardous materials data inputs from HMIS, DSS, BOSS, and DAISY. This information is processed by ERLS to create reports that identify the DoD hazardous material inventories at a location and the characteristics of those inventoried products.

HMIS

- Chemical Composition
- MSDS identification

DSS

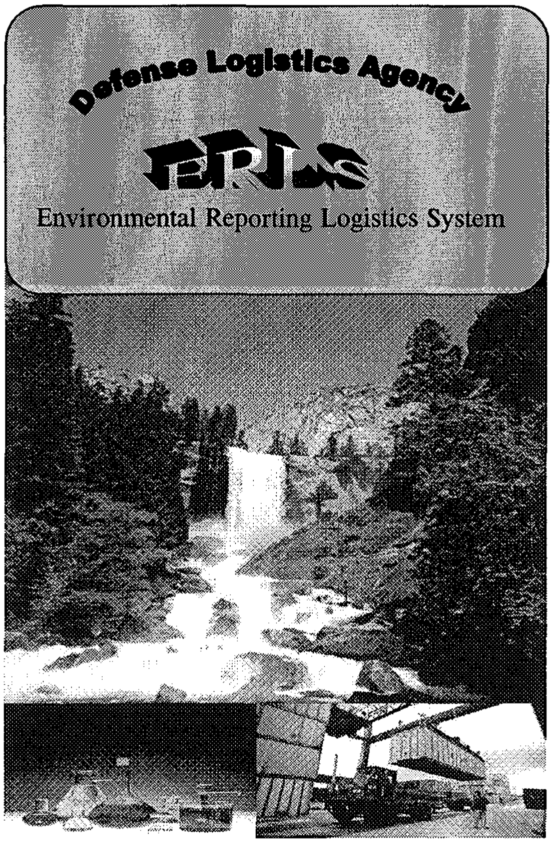
- Support for depot functional business processes

DAISY

- Disposal inventory of DRMOs

BOSS

- Retail supply inventory at depots, DRMO, and inventory control points.



Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Deputy Under Secretary of Defense (Environmental Security)
  Deputy Under Secretary of Defense (Logistics)
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
  Principal Director for Year 2000

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Inspector General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Inspector General, Department of the Navy
Inspector General, Department of the Marine Corps
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force

Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Defense Contract Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
Director Defense Intelligence Agency
Director, Defense Logistics Agency
  Commander, Defense Logistics Information Service
Director, National Security Agency
  Inspector General, National Security Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs
General Accounting Office
  Defense Information and Financial Management Systems, Accounting and Information Management Division
  National Security and International Affairs Division
    Technical Information Center

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Subcommittee on Acquisition and Technology, Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Committee on Science
House Subcommittee on Technology, Committee on Science

Audit Team Members

The Contract Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report, are listed below.

Paul J. Granetto
William C. Gallagher
Mary L. Ugone
James W. Hutchinson
Kenneth L. Stavenjord
Danny B. Convis
Robert A. McGriff
Vanessa S. Adams